FACULDADE DE TECNOLOGIA DE AMERICANA "MINISTRO RALPH BIASI"

Curso Superior de Tecnologia em Segurança da Informação

Rodrigo Silveira da Guarda

Gestão de Continuidade de Negócio e Segurança da Informação

Aliados para segurança e resiliência coorporativa

Americana, SP

2021

FACULDADE DE TECNOLOGIA DE AMERICANA "MINISTRO RALPH BIASI"

Curso Superior de Tecnologia em Segurança da Informação

Rodrigo Silveira da Guarda

Gestão de Continuidade de Negócio e Segurança da Informação

Aliados para segurança e resiliência coorporativa

Trabalho de Conclusão de Curso desenvolvido em cumprimento à exigência curricular do Curso Superior de Tecnologia em Segurança da Informação, sob a orientação do Prof. Dr. Daives Arakem Bergamasco

Área de concentração: Segurança da Informação

Americana, SP.

2021

FICHA CATALOGRÁFICA – Biblioteca Fatec Americana - CEETEPS
Dados Internacionais de Catalogação-na-fonte

G947g GUARDA, Rodrigo Silveira da

Gestão de continuidade de negócios e segurança da informação: aliados para segurança e resiliência corporativa. / Rodrigo Silveira da Guarda. – Americana, 2021.

35f.

Monografia (Curso Superior de Tecnologia em Segurança da Informação) - - Faculdade de Tecnologia de Americana – Centro Estadual de Educação Tecnológica Paula Souza

Orientador: Prof. Dr. Daives Arakem Bergamasco

1 Segurança em sistemas de informação I. BERGAMASCO, Daives Arakem II. Centro Estadual de Educação Tecnológica Paula Souza – Faculdade de Tecnologia de Americana

CDU: 681.518.5

Gestão de Continuidade de Negócio e Segurança da Informação

Aliados para segurança e resiliência coorporativa

Trabalho de graduação apresentado como exigência parcial para obtenção do título de Tecnólogo em Segurança da Informação pelo CEETEPS/Faculdade de Tecnologia – FATEC/ Americana.
Área de concentração: Segurança da Informação

Americana, 26 de junho de 2021.

Banca Examinadora:

_____
Daives Arakem Bergamasco (Presidente)
Doutor
Fatec Americana

_____
MAXWEL VITORINO DA SILVA (Membro)
Mestre
Fatec Americana

_____
ADALBERTO ZORZO (Membro)
Mestre
Fatec Americana

DEDICATÓRIA

Dedico este trabalho aos meus filhos, como modelo de perseverança e fé em busca de seus ideais de vida.

AGRADECIMENTOS

Agradeço primeiro a Deus por ter me mantido na trilha certa durante este projeto de pesquisa com saúde e forças para chegar até o final.

Sou grato à minha família pelo apoio que sempre me deram durante toda a minha vida.

Deixo um agradecimento especial ao meu orientador Prof. Dr. Daives Arakem Bergamasco pelo incentivo e pela dedicação do seu escasso tempo ao meu projeto de pesquisa, que não me deixou desistir em nenhum momento.

Também quero agradecer à Fatec de Americana e a todos os professores do meu curso pela elevada qualidade do ensino oferecido.

RESUMO

Este trabalho tem o objetivo de orientar profissionais de Tecnologia em Segurança da Informação e Gestão de Riscos de Segurança da Informação em ambientes coorporativos. Nesse sentido, conceitua a importância de um Plano de Continuidade de Negócio, importante para resiliência e segurança coorporativa. Também orienta a utilização de frameworks para gestão de tecnologia da informação, como Cobit, ITIL e das normas ABNT NBR ISO para orientação na criação de processos estruturados de Gestão de Continuidade de Negócio.

São demostrados todos os processos de Gestão de Continuidade de Negócio, como: análise de impacto nos negócios; gestão de políticas e estratégias; metodologia para avaliação de risco; gestão de riscos; processos de validação e teste; identificação de incidente; recuperação de desastres; papel da comunicação e gerenciamento de continuidade de negócio e o gerenciamento de resiliência e reputação. O trabalho demostra como funciona cada processo e como executar, consoante às normas técnicas, bem como o plano de validação *check-list* de verificação para melhoria contínua do processo.

Neste estudo são abordadas técnicas extraídas nas normas técnicas ABNT NBR ISO 22301, 22316, 22317, 22320, NBRISO31000 e NBRISO/IEC27005 de segurança de informação. Essas normas especificam os requisitos para planejar, criar, implementar, operar, monitorar, analisar criticamente, manter e melhorar continuamente um sistema de gestão documentado para se preparar, responder e recuperar de eventos destrutivos, bem como mapear e analisar mitigar e documentar riscos inerentes a segurança da informação. Os requisitos especificados são genéricos e que deverão ser aplicáveis a todas as organizações (ou suas partes), independentemente do seu tipo, tamanho e natureza. A extensão da aplicação destes requisitos depende do ambiente operacional e sua complexidade.

Palavras Chave: Gestão de Continuidade de Negócio. Gestão de Riscos de Segurança da Informação. Segurança da Informação.

ABSTRACT

This work aims to guide Information Security Technology professionals and Information Security Risk Management in corporate environments. In this sense, it conceptualizes the importance of a Business Continuity Plan, which is important for corporate resilience and security. It also guides the use of information technology management frameworks, such as Cobit, ITIL and ABNT NBR ISO standards to guide the creation of structured Business Continuity Management processes.

All Business Continuity Management processes are demonstrated, such as: business impact analysis; policy and strategy management; methodology for risk assessment; risk management; validation and testing processes; incident identification; disaster recovery; role of communication and business continuity management and the management of resilience and reputation. The work demonstrates how each process works and how to perform it, according to technical standards, as well as the check-list validation plan for continuous process improvement.

In this study, techniques extracted from the technical standards ABNT NBR ISO 22301, 22316, 22317, 22320, NBRISO31000 and NBRISO/IEC27005 for information security are addressed. These standards specify the requirements for planning, creating, implementing, operating, monitoring, critically analyzing, maintaining and continuously improving a documented management system to prepare, respond to and recover from destructive events, as well as mapping and analyzing, mitigating and documenting inherent risks to information security. The specified requirements are generic and should apply to all organizations (or parts of them), regardless of their type, size and nature. The extent to which these requirements apply depends on the operating environment and its complexity.

Keywords: Business Continuity Management. Information Security Risk Management. Information security.

LISTA DE FIGURAS

FIGURA 1 - Relações de Análise de Impacto nos Negócios..... 15
FIGURA 2 - Visão geral do processo de gestão de riscos..... 19
FIGURA 3 - Processo de gestão de riscos de segurança da informação..... 20
FIGURA 4 - Ciclo de vida de Gestão de Continuidade de Negócio..... 24
FIGURA 5 - Exemplo de *Checklist* para avaliação do PCN (parte 1)..... 28
FIGURA 6 - Exemplo de *Checklist* para avaliação do PCN (parte 2) 29

SUMÁRIO

1 INTRODUÇÃO..... 11
1.1 Considerações iniciais..... 11
1.2 Justificativa..... 11
1.3 Objetivos..... 11
1.4 Estrutura do trabalho..... 12
2 REVISÃO BIBLIOGRÁFICA..... 13
2.1 Gestão de Continuidade do Negócio – BCM..... 13
2.1.1 Políticas e Estratégias..... 13
2.1.2 Análise de Impacto nos Negócios ou Business Impact Analysis – BIA..... 14
2.2 Avaliação de risco..... 16
2.3 Gestão de riscos..... 17
2.3.1 Validação e Teste..... 21
2.3.2 Identificação de Incidente..... 21
2.3.3 Recuperação de Desastres..... 22
2.3.4 Papel da Comunicação e Gerenciamento da Continuidade do Negócio..... 22
2. 4 Gerenciamento de Resiliência e Reputação..... 22
2.5 Estruturando o Documento de Gestão de Continuidade de Negócios.... 23
2.5.1 Documentação do Plano de Continuidade de Negócios (PCN)..... 25
2.5.2 Processos e melhores práticas em tecnologia da informação..... 30
2.5.3 Recuperação de um desastre com a Gestão de continuidade de Negócio. 31
2.5.4 Plano de recuperação de desastres..... 32
CONSIDERAÇÕES FINAIS..... 34
REFERÊNCIAS BIBLIOGRÁFICAS..... 35

1 INTRODUÇÃO

1.1 Considerações iniciais

Hoje as organizações de todos os tamanhos e segmentos estão sendo impactadas e testadas pela pandemia da COVID-19. Há uma grande mobilização para responder e reagir à crise através de ações inovadoras com o objetivo de continuar em diante, mas para isso foi preciso mudar a forma de trabalhar, fazer negócios, consultar médicos etc.

Muitas empresas não tinham ideia de que uma pandemia poderia impactar diretamente seu negócio, outras já tinham um planejamento para lidar com crises e desastres, mas como essa pandemia nenhuma delas estava realmente preparada, as empresas que já possuíam um Plano de continuidade de negócio bem estruturado, treinado, testado tiveram uma retomada rápida as suas atividades.

1.2 Justificativa

A gestão de crises e continuidade dos negócios envolve o estabelecimento de um Sistema de Gestão de Continuidade de Negócios (SGCN), cujo escopo compreende o desenvolvimento e implantação de estratégias, equipes, planos e ações que fornecerão proteção e formas alternativas de operação para uma organização frente aos eventos adversos.

O ambiente computacional de uma empresa é um dos mais importantes para gestão da informação e armazenamento dos dados dos sistemas de gestão, e é imprescindível a criação de planos de continuidade operacional (PCO) e plano de recuperação de desastres (PRD), pois as organizações não podem evitar desastres, mas podem desenvolver planos e ações baseadas em cenários reais para minimizar os efeitos de um desastre. Assim reduzindo o tempo de recuperação do ambiente.

1.3 Objetivo

Este estudo tem como objetivo ilustrar os processos de criação de um Sistema de Gestão de Continuidade de Negócios, demostrando o processo de criação, comunicação, mapeamento, estruturação, teste, e validação, para criar um plano tudo

isso com o foco na continuidade dos negócios e a compreensão dos elementos que fortalecem a resiliência operacional são fatores importantes na sobrevivência do negócio.

1.4 Estrutura do trabalho

Neste estudo são abordadas técnicas extraídas nas normas técnicas ABNT NBR ISO 22301, 22316, 22317, 22320, NBRISO31000 e NBRISO/IEC27005 de segurança de informação. Essas normas especificam os requisitos para planejar, criar, implementar, operar, monitorar, analisar criticamente, manter e melhorar continuamente um sistema de gestão documentado para se preparar, responder e recuperar de eventos disruptivos, bem como mapear e analisar mitigar e documentar riscos inerentes a segurança da informação.

Os requisitos especificados são genéricos e que deverão ser aplicáveis a todas as organizações (ou suas partes), independentemente do seu tipo, tamanho e natureza. A extensão da aplicação destes requisitos depende do ambiente operacional e sua complexidade.

2 REVISÃO BIBLIOGRÁFICA

2.1 Gestão de Continuidade do Negócio- BCM

Gestão de Continuidade do Negócio - BCM (Business Continuity Management) é definido como um plano avançado e de preparação de uma organização para manter as funções de negócio ou restaurar rapidamente após uma crise (ou desastre ter ocorrido, também envolve riscos potenciais como incêndios, enchentes, pandemia, ataques cibernéticos etc.).

Gestores planejam identificar e lidar com crises potenciais mesmo antes que elas aconteçam, criando processos e procedimentos para manter e restaurar o negócio. Em seguida testam esses procedimentos para garantir que eles estejam funcionando devidamente, e analisam periodicamente os processos para certificar que ele esteja atualizado e funcionando como deveriam.

A estrutura de gerenciamento de continuidade de negócios descreve o processo de planejamento para o desenvolvimento de arranjos e procedimentos prévios para permitir que as organizações respondam a um evento de tal maneira que funções de negócios críticas possam continuar dentro dos níveis de interrupção previstos.

2.1.1 Políticas e Estratégias

O gerenciamento de continuidade envolve mais do que a reação a um desastre natural ou ataque cibernético. Ele começa com as políticas de segurança e procedimentos desenvolvidos, testados e usados quando ocorre um incidente. A política define o escopo do programa, as partes principais e a estrutura de gerenciamento. Ele precisa articular porque a continuidade dos negócios é necessária e a governança é fundamental nesta fase.

Saber quem é responsável pela criação e modificação de uma lista de verificação do plano de continuidade de negócios é um componente. A outra é identificar a equipe responsável pela implementação. A governança fornece clareza no que pode ser um momento caótico para todos os envolvidos.

O escopo também é crucial. Ele define o que a continuidade dos negócios significa para a organização. Trata-se de manter os aplicativos operacionais, produtos e serviços disponíveis, dados acessíveis ou locais físicos e pessoas seguras? As empresas precisam ter clareza sobre o que é coberto por um plano, sejam os componentes geradores de receita da empresa, aspectos externos ou algum outro subconjunto da organização total. Funções e responsabilidades também precisam ser atribuídas durante esta fase.

Essas funções podem ser óbvias com base na função do trabalho, ou específicas, devido ao tipo de interrupção que pode ocorrer. Em todos os casos, a política, governança, escopo e funções precisam ser amplamente comunicados e apoiados.

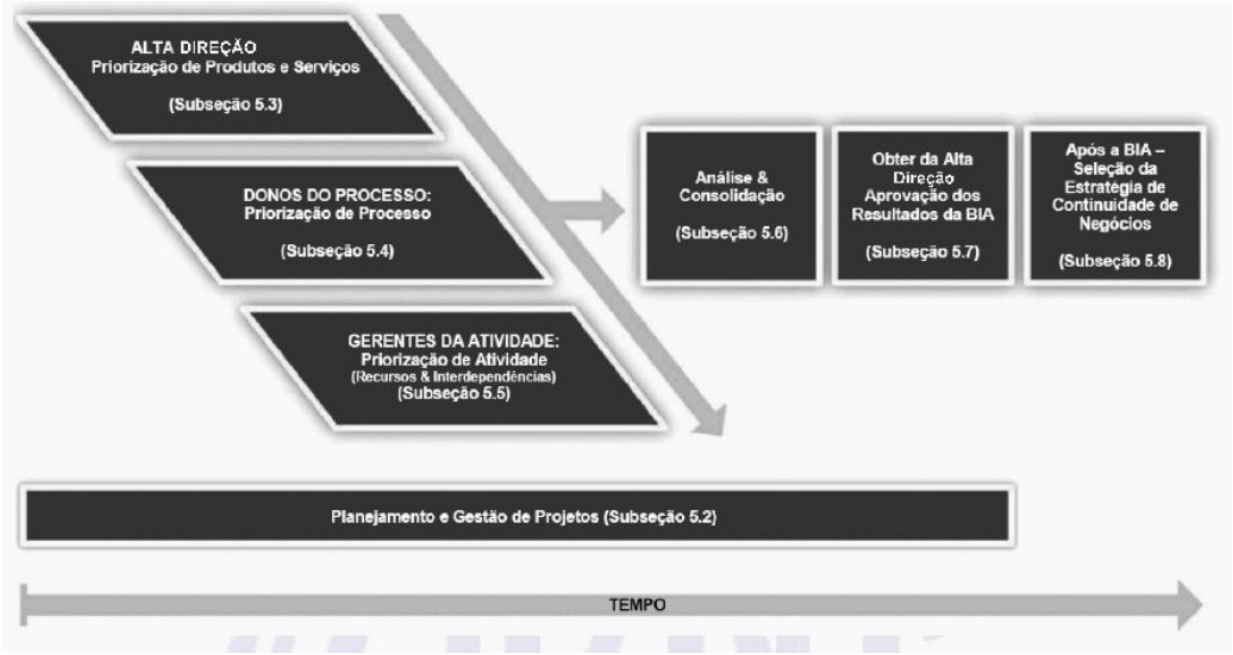
2.1.2 Análise de Impacto nos Negócios ou Business Impact Analysis - BIA

O processo Análise de Impacto nos Negócio – BIA, é detalhado na Especificação Técnica ABNT ISO/TS22317, esta especificação técnica fornece orientações detalhadas para estabelecer, implementar e manter um processo de análise de impacto nos negócios. Nesta especificação, os requisitos de continuidade de negócios têm o mesmo significado que as prioridades, objetivos e metas de continuidade e recuperação (ABNT NBR ISO22301:2013, 8.2.2).

Segundo a TS22317, o processo BIA prioriza os vários componentes organizacionais, de modo que a entrega dos produtos e serviços possa ser retomada em um prazo predeterminado após um incidente disruptivo para a satisfação das partes interessadas, em que os produtos e serviços são priorizados primeiramente, estabelecendo os parâmetros de nível de tempo e serviço para priorização do processo.

A figura 1, abaixo, demonstra as relações de análise de impacto nos negócios.

Figura 1 - Relações de Análise de Impacto nos Negócios



Fonte: ABNT ISO/TS22317 do processo de Análise de Impacto de negócios.

> *..." Se uma organização tiver muitos produtos e serviços para identificar individualmente, a organização pode agrupar produtos e serviços em conjunto quanto tiverem prioridades similares. Por outro lado, pode ser necessário que a organização identifique clientes que, apesar de compartilharem os mesmos produtos e serviços, tenham expectativas no prazo de entrega, ou seu valor para a organização seja diferente."* (ABNT ISO/TS 22317, 2020, ANO, p8)

A avaliação de impacto é um processo de catalogação para identificar os dados que a empresa mantém, onde são armazenados, como são coletados e como são acessados. Determina quais desses dados são mais críticos e qual é a quantidade de tempo de inatividade aceitável se esses dados ou aplicativos estar indisponível. Embora as empresas tenham como objetivo o tempo de atividade de 100%, essa taxa nem sempre é possível, mesmo com sistemas redundantes e recursos de armazenamento.

Essa fase também é o momento em que você precisa calcular seu objetivo de tempo de recuperação, que é o tempo máximo que levaria para restaurar os

aplicativos a um estado funcional no caso de uma perda repentina de serviço. Esse período pode ser chamado de “período máximo tolerável de interrupção (MTPD)”.

Além disso, as empresas devem saber o objetivo do ponto de recuperação, que é a idade dos dados que seria aceitável para os clientes e sua empresa retomarem as operações. Também pode ser considerado o fator de aceitabilidade da perda de dados.

A Alta Direção precisa concordar com a prioridade de produtos e serviços após um incidente disruptivo que pode ameaçar o alcance de seus objetivos. É responsabilidade dela tomar essas decisões pois ela que estabelece os objetivos da organização, tem responsabilidade final de assegurar a continuidade da organização e o atendimento dos seus objetivos, somente ela tem a visão mais ampla de toda organização para determinar as prioridades, e somente ela tem o poder por optar cancelar obrigações contratuais e outras obrigações em circunstâncias excepcionais, e estar ciente das mudanças futuras planejadas e de outros fatores que podem afetar os requisitos de continuidade de negócio.

2.2 Avaliação de risco

Uma organização deve implementar e manter um processo de avaliação de riscos, processo de Gestão de riscos é abordado na ABNT NBR ISO 31000, mas no âmbito da Tecnologia da Informação, a Norma Brasileira para Gestão de Riscos de segurança da informação, é a ABNT NBR ISO/IEC 27005.

> *“Esta Norma fornece diretrizes para o processo de gestão de riscos de segurança da informação de uma organização, atendendo particularmente aos requisitos de um sistema de gestão de segurança da informação (SGSI) de acordo com a ABNT NBR ISO/IEC 27001. Entretanto, esta Norma Internacional não inclui um método específico para a gestão de riscos de segurança da informação. Cabe à organização definir sua abordagem ao processo de gestão de riscos, levando em conta, por exemplo, o escopo do seu SGSI, o contexto da gestão de riscos e o seu setor de atividade econômica. Há várias metodologias que podem ser utilizadas de acordo com a estrutura descrita nesta Norma para implementar os requisitos de um SGSI.”* (ABNT NBR ISO/IEC 27005, vi)

Há várias metodologias que podem ser utilizadas de acordo com a estrutura descrita na ISO/IEC 27005 para implementar os requisitos de um SGSI. Ela é um documento baseado no método de identificação de riscos de ativos, ameaças e vulnerabilidades, que não é mais requerido pela ABNT NBR ISO/IEC 27001. Ela é mais um documento aplicável a gestores e pessoal envolvido com a gestão de riscos de segurança da informação em uma organização e, quando apropriado, em entidades externas que são suporta a essas atividades. (NBR ISO/IEC 27005:2019)

De acordo com a ISO27005 é preciso uma abordagem sistemática de gestão de riscos de segurança da informação é necessária para identificar as necessidades da organização em relação aos requisitos de segurança da informação para criar um sistema de gestão de segurança da informação (SGSI). Para que a segurança lide com os riscos de maneira efetiva e no tempo apropriado, onde quando forem necessários. A Gestão de segurança da informação é um processo contínuo e deve ser aplicado e implementado no cotidiano da organização.

2.3 Gestão de riscos

A Gestão de Riscos é definida com uma das atividades coordenadas para direcionar e controlar uma organização no que se refere ao risco (ABNT NBR ISO/IEC 27001). A gestão de riscos deve ser um processo que inclui a identificação, análise, avaliação, tratamento, aceitação, comunicação, monitoramento e revisão do risco, onde se deve analisar todos os riscos inerentes às atividades de uma organização.

> *"O processo de gestão de riscos de segurança da informação pode ser aplicado à organização como um todo, a uma área específica da organização (por exemplo, um departamento, um local físico, um serviço), a qualquer sistema de informações, a controles já existentes, planejados ou apenas a aspectos particulares de um controle (por exemplo, o plano de continuidade de negócios)."* (ABNT NBR ISO/IEC 27005)

O PDCA (Plan-Do-Check-Act) Plano de melhoria contínua, é um ciclo de análise e melhoria dos processos gerencias necessários para o sucesso de uma organização é usado para área de segurança da informação. Ele deve ser utilizado para estruturar os processos do Sistema de Gestão de Segurança da Informação o

SGSI e alinha os processos de gestão de risco. O PDCA é um processo dividido em quatro etapas: Planejar, Executar, Checar e Agir; são elas:

a) Planejar: inicia com a definição das estratégias e a forma como elas vão ser alcançadas, a definição de políticas, controles e procedimentos para garantir a segurança das informações.

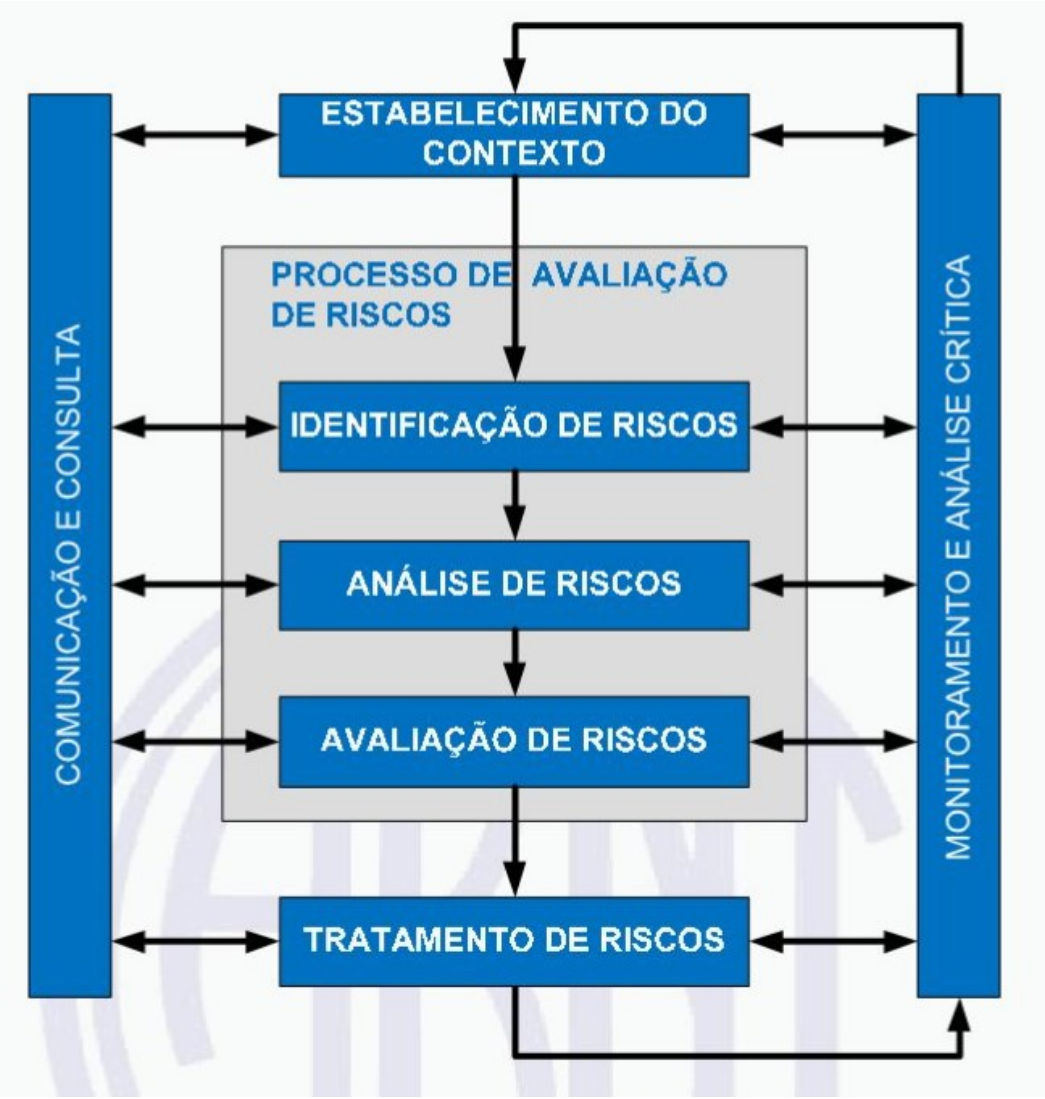
b) Executar: os processos definidos são implementados e executados, também é necessária coleta de informação para próxima etapa, durante essa de execução alinhada com a norma ISO/IEC27005 é implementado o processo de tratamento do risco.

c) Checar: nesta etapa é feita a avaliação dos processos implementados para verificar se o que foi planejado foi realmente executado de forma adequada alcançando as metas estabelecidas no planejamento. Durante este processo são identificados os possíveis desvios de execução e apresentados os resultados para uma análise crítica da alta direção. Está é a etapa em que a norma ISO/IEC27005 se refere ao Monitoramento Continuo e análise crítica do Risco.

d) Agir: nesta etapa são realizadas as ações corretivas e preventivas baseadas na identificação de desvios de execução e nas considerações apresentadas pela alta direção da organização. A norma 27005 orienta manter e melhorar o processo de Gestão de Riscos de Segurança da Informação.

Uma visão do alto nível do processo de gestão de riscos é especificada na ABNT NBR ISO 3100 e apresentado abaixo na figura 2.

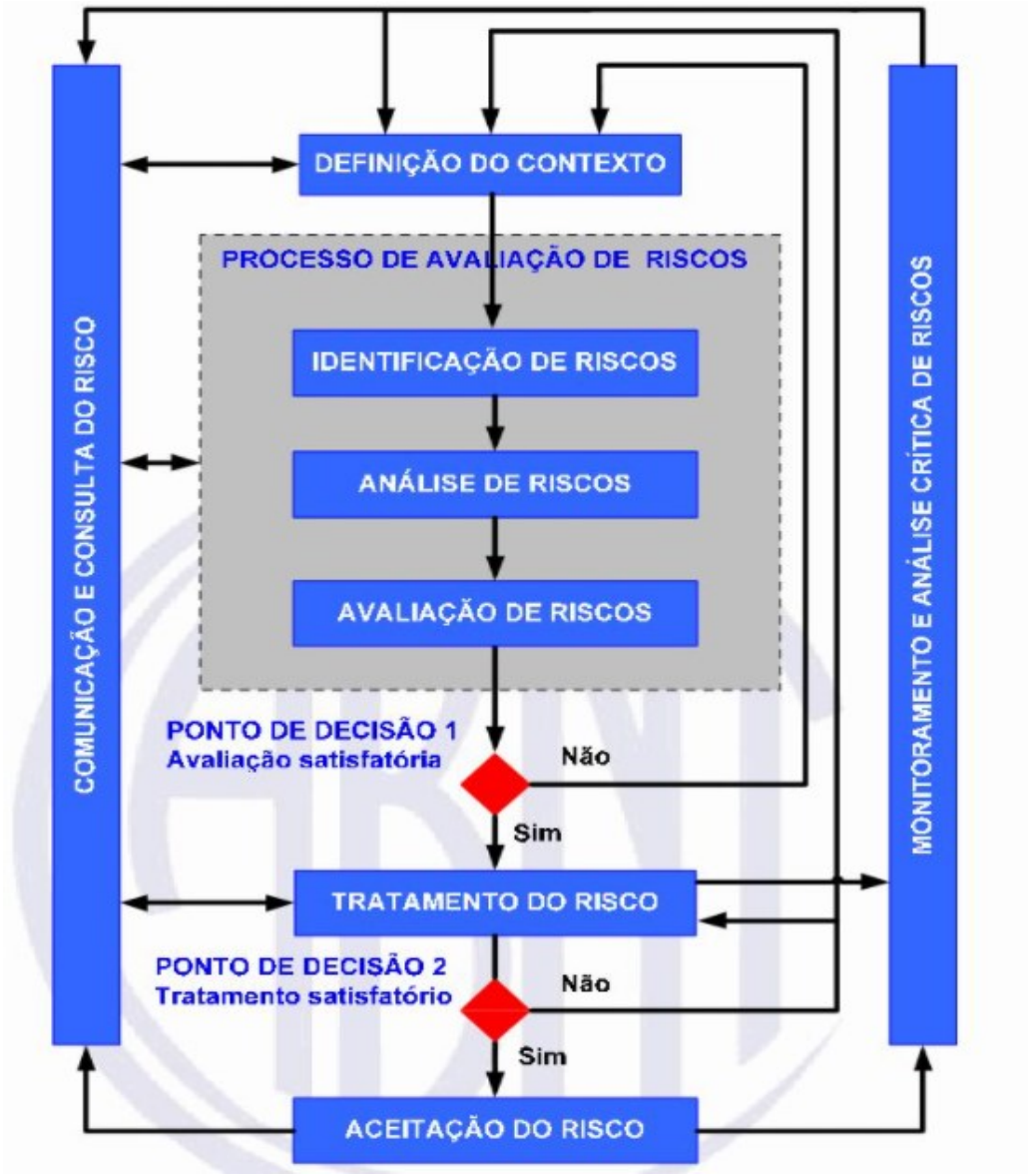
Figura 2 – Visão geral do processo de gestão de riscos



Fonte**: –** Norma ABT NBR ISO/IEC27005, processo de gestão de riscos

Assim, o processo de gestão de riscos de segurança da informação consiste na definição do contexto, processo de avaliação dos riscos, tratamento do risco, aceitação do risco, comunicação e consulta do risco e monitoramento e análise crítica de riscos. A figura 3, a seguir, apresenta como o PDCA é aplicado no processo de gestão de riscos.

Figura 3 – Processo de gestão de riscos de segurança da informação



Fonte: Norma ABT NBR ISO/IEC27005, processo de gestão de riscos

O risco surge de várias formas e, consequentemente, uma análise de impacto nos negócios e uma avaliação de ameaças e riscos devem ser realizadas. As ameaças podem incluir atores mal-intencionados, atores internos, concorrentes, condições de mercado, questões políticas (nacionais e internacionais) e ocorrências naturais. Um componente-chave do seu plano é criar uma avaliação de risco que identifica ameaças potenciais à empresa. A avaliação de riscos identifica a ampla gama de riscos que podem impactar a empresa.

Identificar ameaças potenciais é o primeiro passo e pode ser de longo alcance. Isso inclui: analisar o impacto da perda de pessoal, descobrir mudanças nas preferências do consumidor ou cliente, ter agilidade interna e capacidade de responder a incidentes de segurança com um plano e ter volatilidade financeira.

As empresas regulamentadas precisam levar em consideração o risco de não conformidade, que pode resultar em pesadas penalidades e multas financeiras, maior fiscalização da agência e perda de posição, certificação ou credibilidade. Cada risco precisa ser articulado e detalhado. Na próxima fase, a organização precisa determinar a probabilidade de cada risco acontecer e o impacto potencial de cada um. Probabilidade e potencial são medidas importantes quando se trata de avaliação de risco.

Uma vez que os riscos foram identificados e classificados, a organização precisa determinar qual é sua tolerância ao risco para cada potencialidade. Quais são os problemas mais urgentes e críticos que precisam ser resolvidos? Nesta fase, as soluções potenciais precisam ser identificadas, avaliadas e precificadas. Com essas novas informações, que incluem probabilidade e custo, a organização precisa priorizar quais riscos serão abordados.

Os riscos classificados, então, precisam ser avaliados quanto a quais riscos serão tratados primeiro. Observe que esse processo não é estático. Precisa ser regularmente discutido para levar em conta as novas ameaças que surgem como tecnologias

2.3.1 Validação e Teste

Os riscos e seus impactos precisam ser continuamente monitorados, medidos e testados. Uma vez que os planos de mitigação estejam em vigor, eles também devem ser avaliados para garantir que estão funcionando de forma correta e coesa.

2.3.2 Identificação de Incidente

Com a continuidade dos negócios, definir o que constitui um incidente é essencial. Os eventos devem ser claramente descritos em documentos de política, assim como quem ou o que pode desencadear a ocorrência de um incidente. Essas

ações desencadeadoras devem estimular a implantação do plano de continuidade de negócios conforme definido e colocar a equipe em ação.

2.3.3 Recuperação de Desastres

Qual é a diferença entre continuidade de negócios e recuperação de desastres? O primeiro são os planos abrangentes que orientam as operações e estabelecem políticas. A recuperação de desastres é o que acontece quando ocorre um incidente.

A recuperação de desastre é a implantação das equipes e ações que são acionadas. São os resultados líquidos do trabalho realizado para identificar os riscos e remediá-los. A recuperação de desastres envolve respostas a incidentes específicos, em oposição a um planejamento mais amplo. Depois de um incidente, uma tarefa fundamental é interrogar e avaliar a resposta e revisar os planos de acordo.

2.3.4 Papel da Comunicação e Gerenciamento da Continuidade do Negócio

A comunicação é um componente essencial do gerenciamento da continuidade dos negócios. A comunicação de crise é um componente, garantindo que haja processos transparentes de comunicação com clientes, consumidores, funcionários, equipe sênior e partes interessadas. Estratégias de comunicação consistentes são essenciais durante e após um incidente. As mensagens devem ser consistentes, precisas e provenientes de uma voz corporativa unificada.

O gerenciamento de crises envolve muitas camadas de comunicação, incluindo a criação de ferramentas para indicar o progresso, necessidades críticas e problemas. Os tipos de comunicação podem variar entre os constituintes, mas devem ser baseados nas mesmas fontes de informação.

2. 4 Gerenciamento de Resiliência e Reputação

Os riscos de não ter um plano de continuidade de negócios são significativos. A ausência de preparação significa que a empresa está mal preparada para lidar com questões urgentes. Esses riscos podem deixar uma empresa surpresa e podem levar a outros problemas significativos, incluindo:

a) Tempo de inatividade para servidores, sistemas e aplicativos baseados em nuvem. Mesmo minutos de inatividade podem resultar na perda de receitas substanciais.
b) Perda de credibilidade para reputação e identidade de marca. O tempo de inatividade generalizado, consistente ou frequente pode corroer a confiança dos clientes e consumidores. A retenção de clientes pode despencar.
c) A conformidade regulatória pode estar em risco em setores como serviços financeiros, saúde e energia. Se os sistemas e os dados não estiverem operacionais e acessíveis, as consequências serão graves.

Gerenciar a continuidade dos negócios envolve proteção e integridade de dados, cuja perda pode ser catastrófica. Deve fazer parte da cultura organizacional, com uma abordagem sistemática para o planejamento de continuidade de negócios, as empresas podem agilizar a recuperação de atividades críticas.

2.5 Estruturando o Documento de Gestão de Continuidade de Negócios

A Gestão de Continuidade de Negócios (BCM) é um processo que estabelece uma estrutura estratégica e operacional para: a) Melhorar proativamente a resiliência da organização contra possíveis interrupções; b) Prover uma prática para restabelecer a capacidade de fornecimento de produtos e serviços; c) Obter reconhecida capacidade de gerenciar uma interrupção no negócio, protegendo marca e reputação.

A participação da alta direção é fundamental para garantir que o processo de BCM seja corretamente introduzido, suportado e estabelecido como parte da cultura da organização.

Em escopo macro, na Gestão de Continuidade de Negócios (BCM) são cumpridos os seguintes passos: 1) Elaboração da Análise de Impacto ao Negócio (BIA); 2) Sugestão de Estratégia de Continuidade de Negócios; 3) Elaboração do Plano de Continuidade de Negócios para a área de TI, áreas de negócios e áreas de suporte aos negócios; 4) Implantação do PCO e/ou PRD; 5) Testes e treinamentos periódicos do PCO e/ou PRD; 6) Revisões periódicas do PCN (Plano de Continuidade de Negócios).

O processo de BCM baseado na norma ABNT NBR ISO 22301:2013 é composto de 4 (quatro) etapas.

Figura 4 - Ciclo de vida de Gestão de Continuidade de Negócio

Fonte: https://www.jcu.edu.au/policy/corporate-governance/business-continuity-policy3

A etapa 1 envolve a Análise de Impacto no Negócio (BIA), por meio da: a) Identificação das áreas de negócio; b) Clientes relacionados; c) Sazonalidade quanto as atividades realizadas em períodos de picos críticos; d) Impactos quanto a Imagem, reputação, obrigações legais e monitoramento/segurança; e) Impacto financeiro relacionado a multas e receita (definição por tipo associado); f) Recursos necessários (tecnologia, serviços, fornecedores, pessoas); g) Tempo objetivado de recuperação e Ponto de restauração objetivado; h) Responsabilidades de acionamento de fornecedores / DR. Quanto à Avaliação de Riscos, cabe observar: ameaças, vulnerabilidades e riscos propriamente ditos.

Na etapa 2 é determinada a estratégia de continuidade de negócios, para isso, faz-se necessário levar em consideração o período máximo de interrupção, os custos de implementação da(s) estratégia(s) e as consequências de não se agir. Também é importante considerar os recursos disponíveis quanto a pessoas, instalações, tecnologia, informação, suprimentos e partes interessadas.

A etapa 3 consiste em desenvolver e implementar uma resposta de BCM. Nesse contexto, o plano envolve: a) Resposta a Incidentes; b) Gerenciamento de Crise; c) Continuidade de Negócios; d) Plano de Recuperação de Desastre – PRD,

envolvendo aplicações, dados e infraestrutura; e) Plano de Continuidade Operacional – PCO, envolvendo os recursos; f) Comunicação (mídia, partes interessadas).

Por fim, a etapa 4 é responsável por: a) Programação de testes; b) Manutenção; c) Análise crítica da capacidade de BCM da organização: elencando o resultado de testes e as necessidades das partes interessadas; d) Auditoria (interna ou externa ou autoavaliações).

2.5.2 Documentação do Plano de Continuidade de Negócios (PCN)

Durante o processo de implementação do Plano de Continuidade de Negócios (PCN), são necessários alguns documentos, elencados abaixo:

- Avaliação pelas áreas usuárias p/ identificação de sistemas críticos;
- Definição do *downtime* máximo por aplicação;
- Elaboração do plano de recuperação das aplicações/serviços;
- Definição da priorização dos sistemas quando do acionamento do PCN;
- Definição armazenamento mídias off site;
- Definição das pessoas autorizadas a ativar/desativar o PCN;
- Elaboração/Divulgação do plano de comunicação;
- Elaboração/Divulgação do plano de notificação da crise;
- Definição do time de gerenciamento de crise;
- Elaboração do plano de contatos e lista de fornecedores;
- Mapeamento de TI, onde será mapeada a infraestrutura (hardware/software) de acordo com o escopo.

Ainda, diariamente, faz-se necessária a revisão periódica das documentações de PRD/PCO e do PCN e a utilização de testes periódicos de acionamento da contingência. Durante o Desenvolvimento da Análise de Impacto ao Negócio (BIA), geralmente definida como fase 1, ocorre a realização de entrevistas com as áreas; o levantamento dos clientes impactados, do impacto financeiro, do impacto institucional e o mapeamento de TI, que analisa os riscos e ameaças, atualizando a identificação de riscos, vulnerabilidade e ameaças. Em seguida, são levantadas as

necessidades em contingência e a sugestão de Estratégia de Continuidade de Negócios (CN).

As informações das atividades anteriores serão consideradas como recursos para a definição da Estratégia de Continuidade, que abrange necessidades operacionais e de TI, como: 1) Processos contingenciados; 2) Necessidades de Tecnologia; 3) Necessidades de comunicação; 4) Identificação dos recursos e suprimentos necessários; 5) Métodos de backup; 6) Tipos de Localidades de Recuperação (Site Backup, DR Site).

Em seguida, dá-se início a fase 2, em que ocorre o desenvolvimento do PCN e a implantação do PRD. De modo geral, cada um é explicado abaixo:

a) Plano de Gestão de Crise (PGC): Orienta ações de avaliação do cenário da crise, acionamento das áreas críticas para execução dos planos envolvendo a comunicação de parceiros, fornecedores, clientes-chave e a mídia através do Plano de resposta a emergência (PCI – Plano de Comunicação Interna e PCE – Plano de Comunicação Externa);
b) Plano de Resposta a Incidentes (PRI) / Plano de resposta a emergência cujo conteúdo está voltado aos procedimentos de contenção e/ou limitação de danos ocasionados pela ocorrência de um Incidente;
c) Plano de Contingência Operacional (PCO) / Criação de Procedimento para PCO cujo conteúdo está voltado aos procedimentos alternativos para a continuidade dos Processos/Atividades Críticas até o restabelecimento das operações;
d) Plano de Recuperação de Desastres (PRD) / Processo de Recuperação de Desastres - Clientes cujo objetivo é restabelecer as operações tecnológicas que suportam os negócios, assegurando que as operações críticas possam recomeçar o processamento normal dentro de um espaço de tempo aceitável (RTO);
e) Plano de Teste e Exercício (PTE) / Política de Testes e Exercícios do PCN cujo conteúdo está voltado à validação das atividades/procedimentos que integram os planos, identificando ações corretivas e/ou preventivas, quando necessárias;

f) Conscientização em BCM: Capacitar os funcionários na compreensão dos princípios, conceitos e objetivos da Gestão da Continuidade de Negócios.

É recomendada a utilização de um checklist para avaliação do PCN – Plano de continuidade de negócio, segue abaixo o conceito extraído do Guia de Boas Práticas para Planos de Continuidade de Negócios da Comissão Técnica Regional Sudeste de Governança da ABRAPP de outubro de 2012.

A seguir nas páginas 28 e 29, são apresentadas as figuras 5 e 6 que evidenciam um exemplo de *Checklist* para avaliação do PCN.

Figura 5 - Exemplo de *Checklist* para avaliação do PCN (parte 1)

	Item	*Institucionalizado (sim/não)*	*Avaliação (legenda)*	*Observação*
1	Estabelecimento da estrutura gerencial para iniciar, coordenar, implantar e manter todo o processo de PCN.			
2	Avaliação continua e consequentes ajustes do PCN.			
3	Definição dos responsáveis, e substitutos, com funções e alçadas claramente definidas.			
4	Documentação detalhada sobre as definições de critérios para identificação de processos críticos e as atividades afetadas.			
5	Identificação dos ativos envolvidos nos processos identificados como críticos (mapeamento dos processos).			
6	Identificação da relação entre processos/ atividades, ponderando as dependências de sistemas, de pessoas, finanças entre outros.			
7	Identificação dos eventos que podem gerar interrupção.			
8	Identificação das possibilidades de ocorrência dos eventos de ruptura e seus impactos (eventos/cenários).			
9	Análise dos impactos financeiro, operacional, imagem e legal.			

Fonte: Guia de Boas Práticas para Planos de Continuidade de Negócios da Comissão Técnica Regional Sudeste de Governança da ABRAPP de outubro de 2012.

Figura 6 - Exemplo de *Checklist* para avaliação do PCN (parte 2)

10	Definição do tempo de recuperação para cada atividade identificada como crítica (RTO).			
11	Definição do período máximo de perda ou indisponibilidade de dados (RPO).			
12	Mapeamento dos custos da contingência.			
13	Identificação de medidas que reduzam ou evitem a probabilidade de interrupção.			
14	Identificação de medidas que reduzam o período de interrupção.			
15	Identificação de medidas que limitem o impacto de uma interrupção nos produtos/ serviços críticos.			
16	Identificação de medidas que reduzam o risco e o custo durante o período de interrupção.			
17	Definição do nível das ações de contingência, a partir dos processos/ atividades críticas e eventos/cenários de ruptura. Exemplo: *backup*, site de contingência.			
18	Definição dos recursos necessários (exemplo: pessoas, instalações, TI) para cada nível de ação de contingência.			
19	Definição da estratégia de recuperação (critérios e procedimentos de implementação).			

LEGENDA:
0 – não possui
1 – incipiente / em elaboração / em desenvolvimento
2 – atende parcialmente
3 – em fase de conclusão
4 – atende totalmente

Fonte: Guia de Boas Práticas para Planos de Continuidade de Negócios da Comissão Técnica Regional Sudeste de Governança da ABRAPP de outubro de 2012.

2.5.2 Processos e melhores práticas em tecnologia da informação

O departamento de Tecnologia da Informação é um dos mais importantes departamentos das organizações, pois é um departamento que precisa se manter forte, capacitado, estruturado e atualizado, para manipular dados operacionais e prover informações gerencias a alta direção da organização de uma forma mais rápida, dinâmica e com custos cada vez mais baixos. No intuito de auxiliar na melhora dos processos de negócio e garantir o retorno de investimento foi criado um movimento chamado Governança de TI (MANSUR, 2007).

Frameworks como Cobit, Itil são duas *frameworks* de governança utilizadas para entregar as melhores práticas de gestão de recursos de tecnologia da informação.

O CobiT – *Control Objectives for Information and Releted Technology*, é um guia de melhores práticas criado pela *Information Systems Audit and Control Association* (ISACA) para promover um modelo para gerenciamento da Governança de TI. O COBIT 5 consolida COBIT 4.1, *Val IT* e *Risk IT* em uma única estrutura atuando como uma estrutura corporativa alinhada e interoperável com outros frameworks e padrões. O foco do processo do COBIT é ilustrado por um modelo de processo que subdivide TI em 4 domínios (Planejar e Organizar, Adquirir e Implementar, Entregar e Suportar e Monitorar e Avaliar) e 34 processos em linha com as áreas de responsabilidade de planejar, construir, executar e monitorar. Está posicionado em um nível alto e foi alinhado e harmonizado com outros padrões de TI mais detalhados e boas práticas, tais como COSO, ITIL, BiSL, ISO 27000, CMMI, TOGAF e PMBOK.

O ITIL – *Information Technology Infrastructure Library*, foi criado no final da década de 80 pela Agência Central de Computação e Telecomunicações (CCTA) do Governo do Reino Unido, por diversos proponentes a prestadores de serviços de TI para o governo britânico. Era composto de uma biblioteca com 31 volumes com as melhores práticas para o Gerenciamento de serviços de TI. Em sua versão 4 o ITIL 4 Edition define como primeiro componente chave o sistema de valores de serviço (SVS). ITIL nomeou cinco componentes principais do ITIL SVS. Os conhecidos processos ITIL são agora denominados como práticas. Eles são agrupados como 14 práticas de gerenciamento geral, 17 práticas de gerenciamento de serviços e três práticas de gerenciamento técnico.

2.5.3 Recuperação de um desastre com a Gestão de continuidade de Negócio

Os termos Continuidade de negócios e Recuperação de desastres não são intercambiáveis, embora muitos pareçam pensar o contrário. Recuperação de desastres (DR) versus Continuidade de negócios (BC) são duas estratégias totalmente diferentes, cada uma das quais desempenha um aspecto significativo na proteção das operações de negócios.

Quando se trata de proteger seus dados, é fundamental entender as diferenças e planejar com antecedência. Essas diferenças surgem tanto do uso quanto da aplicação após a ocorrência de uma catástrofe. A continuidade dos negócios consiste em um plano de ação. Ele garante que os negócios regulares continuarão mesmo durante um desastre. A recuperação de desastres é um subconjunto do planejamento de continuidade de negócios. Os planos de recuperação de desastres envolvem a restauração de sistemas de suporte vitais. Esses sistemas são principalmente comunicações, hardware e ativos de TI. A recuperação de desastres visa minimizar o tempo de inatividade dos negócios e foca em fazer com que as operações técnicas voltem ao normal no menor tempo possível.

Continuidade de negócios tem um escopo mais amplo, o gerenciamento de continuidade de negócios se refere aos processos e procedimentos que os associados adotam para garantir que as operações regulares de negócios continuem durante um desastre, isso pode significar a diferença entre sobrevivência e desligamento total. Baseia-se em uma análise implacável e no isolamento de processos críticos de negócios.

Um dos principais benefícios é o foco nos processos de negócios. Você avalia o que deve fazer em caso de desastre. Você articula benefícios versus custos. Este é apenas um gerenciamento de dados sólido, mesmo que a catástrofe nunca ocorra. Portanto, você já decidiu quais funções de negócios são críticas. Você sinalizou o que pode ser suspenso até que se recupere totalmente. Você tem uma lista de prioridades. Por exemplo, você se concentraria apenas em clientes ativos? Quais são suas prioridades para gerenciamento de suprimentos e armazenamento?

As leis federais e estaduais exigem um planejamento formal de recuperação de desastres. Com o planejamento de continuidade de negócios, você reservou seus recursos.

Esses recursos suportam suas funções mais essenciais. Eles incluem qualquer equipamento de suporte, software e estoque necessários para avançar. Você gerencia esse estoque mantendo seu estoque atualizado. Você alterna os suprimentos consumíveis em seu estoque de emergência.

Além disso, você identificou os principais funcionários. Eles sabem o que devem fazer e quando devem fazê-lo. Para cada trabalho que há a fazer, alguém deve ser designado para fazê-lo. Os “executores” designados devem ser qualificados para conduzir os negócios no caso de um desastre. Portanto, o plano deve incluir a prática e atualização do plano conforme necessário.

O plano também deve se concentrar nos clientes e na cadeia de suprimentos. Os fornecedores devem saber que suas faturas de pagamento estão em andamento e prontas para pagamento. Os clientes devem ter certeza de que seus pedidos serão atendidos ou apenas temporariamente atrasados, talvez com um desconto especial.

Finalmente, seu plano de BC deve incluir um processo para substituir e recuperar seus sistemas de TI. Isso contém dados de negócios valiosos. Por exemplo, sua rede foi projetada para backup e recuperação de dados?

2.5.5 Plano de recuperação de desastres

As diretrizes de recuperação de desastres definem os procedimentos para restaurar, no menor tempo possível, as operações de tecnologia da informação em caso de interrupção não programada. Também devem prever os impactos de paralização e o tempo máximo necessário para recuperação das atividades da organização

A recuperação de desastres é um subespaço do planejamento total da continuidade dos negócios. Um plano de DR inclui colocar os sistemas em funcionamento após um desastre. Uma das causas que contribuem para essas falhas de negócios é a falta de um plano por escrito. O plano deve incluir uma análise de impacto nos negócios. Muitas empresas redigem o plano, mas deixam de atualizá-lo, pelo menos anualmente. Por exemplo, quando o desastre natural Furacão Harvey causou inundações inesperadas no interior de Houston. Muitas empresas foram inundadas rapidamente enquanto as pessoas lutavam para evacuar.

As falhas de planejamento relacionadas à tecnologia de infraestrutura também incluem a falta de guias de procedimentos de recuperação e continuidade de

negócios. Como você restaura metodicamente cada aplicativo crítico em sua estrutura de TI? Quanto tempo leva para restaurar seu sistema por meio de backups? Qual é a sua tolerância de ponto de restauração? Um ponto de restauração é um tempo entre o último backup na nuvem e quando o sistema caiu.

Finalmente, se nenhuma pessoa é responsável pela preparação para a recuperação de dados, como isso pode ocorrer? Essa pessoa deve ter autoridade para trabalhar em toda a organização.

As principais estratégias para recuperação são:

1) Recuperação gradual: em que é realizada a reconstrução da infraestrutura começando do zero em outro local físico.
2) Recuperação intermediaria: quando a organização possui um contrato de locação com um fornecedor que possibilita o uso de processamento, armazenamento e conectividade para permitir a execução dos serviços de TI no local do Fornecedor.
3) Recuperação Imediata: a organização possui outro local próprio para que possa executar o suporte aos serviços de TI. São conhecidos como Centro de Processamento de dados Backup, Data Centers Backup, Centros de Alta disponibilidade ou site de Disaster Recovery, em que é possível transferir em pouco tempo os sistemas para outro local, ou mantê-los em sincronizados remotamente pela nuvem e apenas chavear os serviços em caso de falha em um dos datacenters assim mantendo a alta disponibilidade.

CONSIDERAÇÕES FINAIS

O conhecimento nesses processos e normas é imprescindível para um gestor em segurança de da informação ou especialista em segurança da informação pois ele precisará atuar nas etapas de análise, desenvolvimento, teste, implementação e documentação de todos os processos para que o objetivo de se manter o negócio continuamente funcionando minimizando o impacto direto aos colaboradores, aos clientes e reputação da empresa.

Todo esse conjunto de normas e atribuições devem e precisam ser revisadas periodicamente, com os colaboradores e clientes chaves dos serviços relacionados para a continuidade. Assim mantendo a resiliência e a entrega de valor agregado mesmo em tempos de crises.

O Processo de criação do Plano de Continuidade de negócio ajuda a empresa a conhecer melhor seu funcionamento, seus processos, pessoas, produtos e colaboradores chaves para continuidade do negócio. Ajuda a compreender os riscos envolvidos ajuda a identificar vulnerabilidades, falhas de segurança, e falha em processo que podem impactar na perda de dados, ativos e clientes.

Este estudo me permitiu conhecer melhor os processos de gestão de continuidade de negócio, e a conhecer melhor o processo de gerenciamento de risco utilizado para implementação de um plano de continuidade de negócios, em todas duas etapas, entre a criação de documentos durante o processo de criação do plano de continuidade de negócio.

Outro ponto é que a segurança da informação não foi somente um processo de tecnologia, e sim uma chave fundamental no processo, e que todos os departamentos de uma organização devem estar comprometidos com a proteção da informação, pois qualquer falha pode gerar uma impossibilidade de realizar adequadamente as suas operações resultando em prejuízos financeiros, operacionais e de imagem.

Espero que este trabalho seja uma fonte de referência para aprimoramento dos planos de continuidades de negócio, como fonte para estruturação desses processos de gerenciamento de risco, para profissionais de tecnologia da informação, gestores e demais envolvidos nos processos produtivos e da alta direção.

REFERÊNCIAS BIBLIOGRÁFICAS

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS – ABNT **NBR ISO 22301**: Segurança e resiliência – Sistemas de gestão de continuidade de negócios – Requisitos. 2020. 24p.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS – ABNT **NBR ISO 22313**: Segurança e resiliência – Sistemas de gestão de continuidade de negócios – Orientações para uso da ABNT NBR ISO 22301. 2020. 63p.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS – ABNT **NBR ISO 22316**: Segurança e resiliência — Resiliência organizacional — Princípios e atributos. 2020. 11p.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS – ABNT **ISO/TS 22317** (Segurança da sociedade — Sistemas de gestão de continuidade de negócios — Diretrizes para análise de impacto nos negócios (BIA). 2020. 31p.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS – ABNT **NBR ISO 22320**: Segurança e resiliência – Sistemas de gestão de continuidade de negócios – Diretrizes para gestão de Incidentes. 2020. 22p.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS – ABNT **ISO/IEC 27001**: Tecnologia da informação — Técnicas de segurança — Sistemas de gestão da segurança da informação — Requisitos. 2013. 30p

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS – ABNT **ISO/IEC 27005**: Tecnologia da informação – Técnicas de segurança – Gestão de riscos de segurança da informação. 2019. 66p

AXELOS Limited. 4.3 **The ITIL guiding principles**. *ITIL Foundation, ITIL 4 edition*. [S.l.]: Editora: TSO The Stationery Office, 2019.

BUSINESS CONTINUITY POLICY. Disponível em https://www.jcu.edu.au/policy/corporate-governance/business-continuity-policy3. *www.isaca.org*. Acesso em: 25 out. 2020.

FAGUNDES, Eduardo. **Disaster Recovery Plan (DRP)** Disponível em <https://efagundes.com/artigos/disaster-recovery-plan-drp/ > Acesso em: 20 out. 2020.

GUIA DE BOAS PRÁTICAS PARA PLANOS DE CONTINUIDADE DE NEGÓCIOS. Disponível em < https://biblioteca.sophia.com.br/terminal/9147/acervo/detalhe/19097?guid=1623108360592&returnUrl=%2fterminal%2f9147%2fresultado%2flistar%3fguid%3d1623108360592%26quantidadePaginas%3d1%26codigoRegistro%3d19097%2319097&i=1 > Acesso em: 27 out. 2020.

ISO PUBLISHES NEW STANDARD FOR BUSINESS CONTINUITY MANAGEMENT Disponível em: <https://www.iso.org/news/2012/06/Ref1587.html> Acesso em: 20 out. 2020.

MANSUR, R **Governança de TI**. São Paulo: Brasport,2007.